

Form AEC-489
(6-67)

U. S. ATOMIC ENERGY COMMISSION
AEC MANUAL

TRANSMITTAL NOTICE

Chapter 2703 SECURITY OF AUTOMATIC DATA PROCESSING SYSTEMS

SUPERSEDED:

Number

Date

Chapter _____

Page _____

Appendix _____

TRANSMITTED:

Number

Date

TN 2700-7

Chapter 2703 (complete) 3/2/71

Page _____

Appendix _____

REMARKS:

This new chapter sets forth the policy, objective, responsibilities, authorities, and basic requirements for the safeguarding of classified data processed or classified information produced by automatic data processing systems.

U.S. ATOMIC ENERGY COMMISSION
AEC MANUAL

Volume: 2000 Security
Part : 2700 Communications, Technical, and Computer Security

AEC 2703-01
S

Chapter 2703 SECURITY OF AUTOMATIC DATA PROCESSING SYSTEMS

2703-01 POLICY

Classified data processed and classified information produced by an automatic data processing (ADP) system operated by the AEC or its contractors shall be safeguarded consistent with their classification and content.

2703-02 OBJECTIVE

To assure that classified data processed and classified information produced by an ADP system are appropriately safeguarded and disseminated only to authorized personnel.

2703-03 RESPONSIBILITIES AND AUTHORITIES

031 The General Manager or the Deputy General Manager:

- a. authorizes AEC Headquarters employees to have access to AEC or AEC contractor originated Top Secret production rate, stockpile quantity, or transfer data processed or information produced by an ADP system. (Such access may also be authorized as provided in 032, 033, and 036, below.)
- b. approves the transmission of AEC or AEC contractor originated Top Secret production rate, stockpile quantity, or transfer data processed or information produced by an ADP system to personnel of Government agencies other than the Department of Defense.

032 The Assistant General Manager for Development and Production authorizes access to all Top Secret production rate or stockpile quantity data processed or information produced by an ADP system in the fields of special nuclear materials or other special products. (Access to such data or information by certain employees may be authorized by the Assistant General Manager for Military Application and the Director, Division of Production, as specified in 033 and 036, below.)

033 The Assistant General Manager for Military Application:

- a. with regard to Top Secret production rate,

stockpile quantity, or transfer data or information relating to weapons or weapon components processed or produced by an ADP system:

- (1) authorizes access by Managers of Field Offices in instances in which the Division of Military Application has programmatic responsibility for the activity in the field office involved.
 - (2) approves transmission requests where the sender does not know whether the recipient is authorized to receive the data or information to be transmitted:
 - (a) between jurisdictions of different field offices, or
 - (b) between field offices and Headquarters divisions or offices.
 - (3) obtains approval from the General Manager for transmission to Government agencies other than the Department of Defense.
- b. authorizes access by employees within the Division of Military Application to Top Secret production rate, stockpile quantity, or transfer data or information relating to weapons, weapon components, special nuclear materials, or other special products processed or produced by an ADP system.
 - c. authorizes the transmission, over communication circuits or cryptographic systems previously approved by the Director, Division of Security, of Top Secret production rate, stockpile quantity, or transfer data or information relating to weapons and weapon components processed or produced by an ADP system to civilian employees of the Department of Defense, its contractors, or members of the Armed Forces.
 - d. authorizes the transmission of weapon data other than Top Secret production rate, stockpile quantity, or transfer data processed or information produced by ADP systems to AEC and AEC contractors, the Department of Defense, the National Aeronautics and Space Administration, their contractors or subcontractors, the Armed Forces, or other Government agencies.

Approved: March 2, 1971

AEC 2703-034

SECURITY OF AUTOMATIC DATA PROCESSING SYSTEMS

034 The Director, Division of Security:

- a. develops and establishes policies, standards, and procedures for the protection of classified data processed or classified information produced by ADP systems.
- b. provides advice and assistance on the control of classified data processed and classified information produced by ADP systems.
- c. represents the AEC before other governmental agencies and organizations concerning the security aspects of ADP systems.
- d. approves exceptions to and deviations from the provisions of this chapter and its appendix after coordination with concerned Headquarters divisions and offices.
- c. with respect to ADP systems processing classified data or producing classified information involving interconnected equipment of (1) one field office or its contractors and another field office or its contractors, or (2) one field office or its contractors and an outside agency or its contractors:
 - (1) concurs in ADP security proposals.
 - (2) approves the selection, acquisition, distribution, and safeguarding of all ADP access controls, as appropriate, in coordination with concerned Headquarters divisions and offices, field offices, or outside agencies.
- f. reviews ADP security proposals for ADP systems processing classified data or producing classified information of one field office or its contractors.
- g. maintains general descriptions of AEC and AEC contractor written software security measures containing the information specified in appendix 2703, annex D.
- h. evaluates alleged or actual compromises of classified data processed or classified information produced by ADP systems after coordination with the appropriate Headquarters divisions or offices and otherwise assures that necessary action is taken.
- i. with respect to the Headquarters Office and security facilities under Headquarters-administered contracts:
 - (1) assures that classified data processed and classified information produced by ADP systems are safeguarded in

accordance with this chapter and its appendix.

- (2) evaluates and approves ADP security proposals with respect to ADP systems processing classified data or producing classified information regardless of whether or not they involve interconnected equipment between (a) AEC Headquarters and a field office or its contractors or (b) AEC Headquarters and an outside agency or its contractors.
 - (3) approves the selection, acquisition, distribution, and safeguarding of all ADP access controls, as appropriate, in coordination with concerned Headquarters divisions and offices, field offices, or outside agencies.
 - (4) assures that ADP system integrity studies are conducted and evaluated and remedial action taken or countermeasures developed prior to permitting a system to process classified data or produce classified information. Similar assurances shall be obtained if there are any changes in the system configuration which may affect related security measures.
- j. assures that a thorough search is conducted for classified data or classified information unaccounted for and takes necessary action including action to prevent recurrence in regard to compromised or possibly compromised classified data processed or classified information produced by an ADP system.
 - k. approves degaussing methods and equipment used to destroy recorded classified data or classified information.

035 The Director, Division of Management Information and Telecommunications Systems, exercises Headquarters direction and coordination over COMSEC installations, operations and maintenance for AEC and its contractors, as set forth in AECM 0270, "Telecommunications."

036 The Director, Division of Production:

- a. with regard to Top Secret production rate or stockpile quantity data or information in the field of special nuclear materials or other special products processed or produced by an ADP system,
 - (1) authorizes access by Managers of Field Offices in instances in which the

Approved: March 2, 1971

SECURITY OF AUTOMATIC DATA PROCESSING SYSTEMS

AEC 2703-037

- Division of Production has programmatic responsibility for the activity in the field office involved.
- (2) approves transmission requests where the sender does not know whether the recipient is authorized to receive the classified data or classified information to be transmitted:
 - (a) between jurisdictions of different field offices.
 - (b) between field offices and Headquarters divisions or offices.
 - (3) obtains approval from the General Manager for transmission to Government agencies other than the Department of Defense.
- b. authorizes access by employees within the Division of Production to Top Secret production rate, stockpile quantity, or transfer data or information relating to weapons, weapon components, special nuclear materials, or other special products processed or produced by an ADP system.

037 Heads of Divisions and Offices, Headquarters:

- a. safeguard classified data processed and classified information produced by an ADP system in accordance with this chapter and its appendix.
- b. with respect to ADP systems processing classified data or producing classified information (regardless of whether or not they involve interconnected equipment) assure that an ADP security proposal is submitted to the Director, Division of Security.
- c. authorize AEC and AEC contractor personnel to have access to classified data processed or classified information produced by an ADP system over which they have primary responsibility.
- d. authorize the reproduction of recorded or printed Top Secret or Secret data processed or information produced by an ADP system, other than that incidental to normal data processing operations, where the originator of the data or information is not known and they have primary responsibility for the data or information.
- e. notify the Director, Division of Security, of alleged or actual compromises of classified data processed or classified information produced by ADP systems and assure that

- necessary action, including action to prevent recurrence, is taken.
- f. authorize, after compliance with the provisions of AECM 2701, the electrical transmission of:
 - (1) classified data or classified information originated by AEC or AEC contractor employees, processed or produced by an ADP system, other than (a) weapon data, or (b) Top Secret production rate, stockpile quantity, or transfer data or information to other Government agencies and their contractors subject to reviews indicated in 033 and 036 above.
 - (2) Top Secret production rate, stockpile quantity, or transfer data processed or information produced by an ADP system:
 - (a) between different Headquarters divisions or offices,
 - (b) between a Headquarters division or office and a field office, where it is known that the recipient is authorized to receive the data or information.
 - g. except as specified in 033 b. and 036 b., above, request authorization from the General Manager or Deputy General Manager, or the Assistant General Manager for Development and Production, in accordance with 031 and 032, above, for access by employees within their divisions or offices to Top Secret production rate, stockpile quantity, or transfer data processed or information produced by an ADP system.
 - h. forward general descriptions of AEC and AEC contractor written software security measures containing the information specified in appendix 2703, annex D, to the Director, Division of Security.
 - i. request approval of:
 - (1) the Assistant General Manager for Military Application to transmit weapon data processed or information produced by an ADP system to AEC or AEC contractors, the Department of Defense, the National Aeronautics and Space Administration, their contractors or subcontractors, the Armed Forces, or other Government agencies.
 - (2) the Assistant General Manager for

AEC 2703-038

SECURITY OF AUTOMATIC DATA PROCESSING SYSTEMS

- Military Application, as indicated in 033, above, to transmit Top Secret production rate, stockpile quantity, or transfer data processed or information produced by an ADP system to the Department of Defense, its contractors, or members of the Armed Forces.
- (3) the Assistant General Manager for Military Application, or the Director, Division of Production, as indicated in 033 and 036, above, for the transmission of Top Secret production rate, stockpile quantity, or transfer data processed or information produced by an ADP system:
 - (a) between different Headquarters divisions or offices, or
 - (b) between a Headquarters division or office and a field office, where the sender does not know whether the recipient is authorized to receive the data or information.
 - j. request the Assistant General Manager for Military Application, or the Director, Division of Production, to obtain the General Manager's approval for the transmission of Top Secret production rate, stockpile quantity, or transfer data processed or information produced by an ADP system to Government agencies other than the Department of Defense.
 - k. request the Director, Division of Security, to approve degaussing methods and equipment used to destroy recorded classified data or classified information.
 - l. appoint an ADP security officer and necessary alternates at each ADP center processing classified data or producing classified information and assure that they perform the duties listed in appendix 2703, annex C.
 - m. authorize, as provided in 031, 032, 033, and 036, above, AEC and AEC contractor employees to have access to classified data processed or classified information produced by an ADP system over which they have primary responsibility.
 - n. with respect to ADP systems processing classified data or producing classified information involving interconnected equipment of (1) one field office or its contractors and another field office or its contractors or (2) one field office or its contractors and an outside agency or its contractors:
 - (1) evaluate and submit ADP security proposals to the Director, Division of Security, for concurrence.
 - (2) request ADP access controls, as appropriate, from the Director, Division of Security, and safeguard their use and disposition.
 - o. with respect to ADP systems processing classified data or producing classified information of one field office or its contractors:
 - (1) evaluate and submit ADP security proposals to the Director, Division of Security, for review prior to granting approval.
 - (2) approve the selection, acquisition, distribution, and safeguarding of all ADP access controls.
 - p. assure that ADP system integrity studies are conducted and evaluated and remedial action taken or countermeasures developed prior to permitting a system to process classified data or produce classified information. Similar assurances shall be obtained if there are any changes in the system configuration which may affect related security measures.
 - q. approve the appointment of an ADP security officer and necessary alternates at each ADP center processing classified data or producing classified information and assure that they perform the duties listed in appendix 2703, annex C.
 - r. forward general descriptions of AEC and AEC contractor written software security measures containing the information specified in appendix 2703, annex D, to the Director, Division of Security.
 - s. authorize, as provided in 031, 032, 033, and 036, above, AEC and AEC contractor employees to have access to classified data processed or classified information produced by an ADP system over which they have primary responsibility.
 - t. authorize the reproduction of recorded or printed Top Secret or Secret data processed or information produced by an ADP

038 Managers of Field Offices:

- a. safeguard classified data processed and classified information produced by an ADP system in accordance with this chapter and its appendix.

SECURITY OF AUTOMATIC DATA PROCESSING SYSTEMS

AEC 2703-04

- system, other than that incidental to normal data processing operations, where the originator is not known and they have primary responsibility for the data or information.
- i. notify the Director, Division of Security, of alleged or actual compromises of classified data processed or classified information produced by ADP systems and assure that necessary action, including action to prevent recurrence is taken.
 - j. authorize, after compliance with the provisions of AECM 2701, the electrical transmission of:
 - (1) classified data or classified information originated by AEC or AEC contractor employees, processed or produced by an ADP system, other than (a) weapon data, or (b) Top Secret production rate, stockpile quantity, or transfer data or information to other Government agencies and their contractors subject to reviews indicated in 033 and 036, above.
 - (2) Top Secret production rate, stockpile quantity, or transfer data processed or information produced by an ADP system:
 - (a) within their respective field offices,
 - (b) between field offices, or
 - (c) from their respective field offices to Headquarters divisions and offices,
 where the sender knows that the recipient is authorized to receive the data or information.
 - k. request approval of:
 - (1) the Assistant General Manager for Military Application to transmit weapon data processed or information produced by an ADP system to AEC or AEC contractors, the Department of Defense, the National Aeronautics and Space Administration, their contractors or subcontractors, the Armed Forces, or other Government agencies.
 - (2) the Assistant General Manager for Military Application, as indicated in 033, above, to transmit Top Secret production rate, stockpile quantity, or transfer data processed or information produced by an ADP system to the Department of Defense, its contractors, or members of the Armed Forces.
 - (3) the Assistant General Manager for Military Application, or the Director, Division of Production, as indicated in 033 and 036, above, to transmit Top Secret production rate, stockpile quantity, or transfer data processed or information produced by an ADP system:
 - (a) between jurisdictions of different field offices, or
 - (b) between their respective field offices and Headquarters divisions or offices,
 where the sender does not know whether the recipient is authorized to receive the data or information.
 - l. request the Assistant General Manager for Military Application, or the Director, Division of Production, to obtain the General Manager's approval for the electrical transmission of Top Secret production rate, stockpile quantity, or transfer data processed or information produced by an ADP system to Government agencies other than the Department of Defense.
 - m. assure that a thorough search is conducted for classified data or classified information unaccounted for and take necessary action including action to prevent recurrence in regard to compromised or possibly compromised classified data processed or classified information produced by an ADP system.
 - n. request the Director, Division of Security, to approve degaussing methods and equipment used to destroy recorded classified data or classified information.

2703-04 DEFINITIONS

(For Purposes Of This Chapter)

041 Automatic Data Processing (ADP)—data processing performed by a system of electronic or electrical machines including input, processing, and output operations.

042 ADP Access Controls—techniques (e.g., a combination of a user identity code and an information identity code or a file management system) which incorporate security measures to verify effectively a person's identity and authorization to have access to classified data or classified information.

AEC 2703-043

SECURITY OF AUTOMATIC DATA PROCESSING SYSTEMS

043 ADP Center—one or more rooms or a building containing the main elements of an ADP system.

044 ADP Security Proposal—a proposal which outlines an ADP system and the security measures to safeguard classified data processed or classified information produced by the system.

045 ADP System—the interacting of procedures, processes, methods, personnel, and ADP equipment to perform a series of data processing operations either manually or automatically.

046 Classified Data—Restricted Data, Formerly Restricted Data, or other data being processed by an ADP system which requires safeguarding in the interest of national defense.

047 Classified Information—Restricted Data, Formerly Restricted Data, or other information produced by an ADP system which requires safeguarding in the interest of national defense.

048 Compromise—the disclosure of classified data or classified information to persons who are not authorized to receive such data or information.

049 Data—a representation of facts or concepts in a manner suitable for processing by an ADP system.

0410 Information—a representation of facts or concepts produced by an ADP system.

0411 Information Identity Code—a classified string of at least five alphanumeric characters which permits a user access to classified data processed or classified information produced by an ADP system. This code may be assigned at the program level, file level, or record level.

0412 Interconnected Equipment—equipment so coupled together as to permit the transfer of data or information.

0413 Production Rate Data or Information:

- a. data or information relating to the capacity to produce or actual production of:
 - (1) weapons and weapon components.
 - (2) plutonium, tritium, or uranium enriched in the isotope 233.
 - (3) special products other than special nuclear materials.

- (4) uranium enriched in the isotope 235 for the period prior to January 1, 1967.

- b. data or information relating to the actual production of uranium enriched in the isotope 235 when identified with a specific classified program.

0414 Software Security Measures—those computer programs and routines which protect data or information, including classified data processed or classified information produced by an ADP system.

0415 Stockpile Quantity Data or Information—data or information relating to the numbers of weapons, weapon components, special nuclear materials, or other special products stored and available for use.

0416 System Integrity Study—an examination and analysis of an ADP system's security measures to determine whether or not any deliberate attempt by personnel or failure of system components could adversely affect the common defense and security.

0417 Transfer Data or Information—data or information relating to the transfer of custody of weapons from the Atomic Energy Commission to the Department of Defense.

0418 User Identity Code—a classified string of at least five alphanumeric characters which permits a user access to an ADP system processing classified data or producing classified information.

0419 Weapon Data—classified data or classified information concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of atomic weapons or components thereof, including such data or information incorporated in or relating to nuclear explosive devices.

2703-05 BASIC REQUIREMENTS

051 Applicability. This chapter and its appendix apply to Headquarters divisions and offices and field offices, and shall be applied to AEC contractors, including subcontractors.

052 Coverage. This chapter and its appendix:

- a. cover the safeguarding of classified data processed or classified information produced by AEC and AEC contractor and

SECURITY OF AUTOMATIC DATA PROCESSING SYSTEMS

AEC 2703-053

- subcontractor ADP systems when either processing classified data or producing classified information only or when manipulating classified and unclassified data or information concurrently.
- b. do not cover the technical security measures applicable to ADP systems.
- c. do not cover the AEC's Secure Automatic Data Information Exchange message and circuit switching functions.
- d. do not cover the processing, producing or handling of classified foreign intelligence data or information.

053 Appendix 2703. Appendix handbook 2703 contains security procedures and requirements applicable to the processing of classified data or the producing of classified information by an ADP system.

054 Prohibitions. No person, other than a member of a systems integrity study team, shall attempt to penetrate or modify an ADP system's security measures so as either to compromise classified data or classified information or to negate or bypass the system's security measures, except as authorized in writing by the manager of a field office, the Director, Division of Security, or higher authority.

055 References

- a. AECM 0270, "Telecommunications," for additional information regarding the protection of cryptographic equipment and information and the preparation of telecommunication proposals.
- b. AECM 0851, "Automatic Data Processing Standards."
- c. AECM 2001, "Security Survey and Facility Approval," for procedures regarding the conduct of security surveys and the granting of facility approvals.
- d. AECM 2101, "Control of Classified Information," for basic procedures and requirements regarding access to classified information.
- e. AECM 2105, "Control of Classified Documents," for basic procedures and

- requirements regarding the control of classified documents.
- f. AECM 2108, "Weapon Data," for additional information regarding security controls required for weapon data information.
- g. AECM 2201, "Security Education and Training," for procedures and standards for special security instruction or lectures.
- h. AECM 2301, "Personnel Security Program," for basic procedures and requirements regarding personnel security.
- i. AECM 2401, "Physical Protection of Classified Matter and Information," for basic procedures and requirements regarding the physical protection of classified matter and classified information in an ADP system.
- j. AECM 2501, "Control of Visits," for basic procedures and requirements regarding classified and unclassified visits.
- k. AECM 2601, "Violations of Laws of Security Interest," for reporting of alleged or suspected violations of law and losses of classified documents outside a security area.
- l. AECM 2701, "Communications Security," for basic security procedures and requirements relating to secure communication centers.
- m. AECM 2702, "Technical Security" (to be issued), for basic procedures and requirements regarding technical security measures applicable to an ADP system processing classified data or producing classified information.
- n. AECM 3401, "Classification," for basic procedures and requirements regarding the classification and declassification of data or information.
- o. AECM 6301, "General Design Criteria," for information regarding the design of ADP centers.

2703-06 NATIONAL EMERGENCY APPLICATION

The provisions of this chapter and its appendix shall remain in effect during a national emergency, as defined in AECM 0601-04.